

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR LETTERS PATENT

**Enterprise Management of
Public Instant Message Communications**

Inventors:

Ryan W. Battle

Kenneth Fern

Peter Ollodart

Austina De Bonte

Yikang Xu

ATTORNEY'S DOCKET NO. MS1-1709US

1 **TECHNICAL FIELD**

2 [0001] Embodiments of this invention relate to instant messaging, and more
3 specifically to enabling enterprise management of public instant message
4 communications.

5
6 **BACKGROUND**

7 [0002] Instant messaging (IM) has become a popular means of communication
8 that, unlike email, enables users to engage in real-time digital conversations. Due
9 to the ease with which digital communication can occur using instant messaging,
10 some companies have begun allowing their employees to communicate company
11 information via IM. As with email, many companies desire the ability to log the
12 content of instant message communications in which their employees participate.
13 This may be achieved for instances in which two employees of the same company
14 participate in an instant message conversation while both logged into an instant
15 messaging application that is provided by a company server. For example, a
16 company may have Microsoft's Live Communication Server installed on a
17 company network, which then enables communication between clients connected
18 to the network using, for example, Microsoft's Windows Messenger. For example,
19 two employees may log onto the company network using their computers at work
20 or through a virtual private network (VPN) connection and use Microsoft's
21 Windows Messenger to communicate with each other via instant messaging.
22 Because the IM communication is enabled using software on the company
23 network, such communication may be logged using additional software installed
24 on the same network.

1 **[0003]** As described above, companies have the ability to log IM
2 communications if all of the conversation participants are logged into the company
3 network. This is insufficient in many cases, however, due to the fact that
4 employees may be communicating with clients at other companies or may be
5 wanting to communicate via IM from locations other than work, such as from
6 home or while on travel, such as at an Internet kiosk in an airport. In such a
7 scenario, an employee may log into an IM client, such as MSN Messenger, that is
8 available over the Internet and participate in IM conversations as an employee of
9 the company, but there is no way for the company to record a log of the
10 conversation or to apply corporate policies in regard to the employee establishing
11 the public IM connection. This is of great concern, especially in industries such as
12 finance or healthcare, where communications by employees representing a
13 company may be confidential or otherwise sensitive.

14 **[0004]** In addition to real-time digital conversations, many public IM services
15 also provide the ability for two or more users connected to the public IM service to
16 establish direct point-to-point connections (also commonly referred to as peer-to-
17 peer connections). A point-to-point connection enables the users to exchange files
18 and other data directly, without going through the public IM service.

19 **[0005]** Point-to-point communications raise an additional level of concern for
20 companies in that a company has no control over what data an individual may be
21 sharing while representing themselves as a company employee (via a user ID
22 associated with the company).

23 **[0006]** Accordingly, a need exists for a company to have the ability to log
24 instant message conversations that a user participates in while logged in as a
25 company employee, regardless of whether or not the user is connected through a

1 company controlled network. Alternatively, or additionally, a need exists for a
2 company to have the ability to restrict participation in instant message
3 conversations by employees who log into an instant message server from outside
4 of a company controlled network. Furthermore, a need exists for companies to
5 control whether or not their employees are allowed to participate in point-to-point
6 communications, as enabled through an instant messaging client application.

7 8 **SUMMARY**

9 **[0007]** Multiple embodiments for enabling enterprise management of public
10 instant message (IM) communications are described. In a particular embodiment,
11 public instant message communications in which a user associated with a
12 particular domain participates are logged by a public instant message service. The
13 logged data may then be transmitted to a server associated with the domain.

14 **[0008]** In another embodiment, user requests to connect to a public instant
15 message server are redirected to an enterprise instant message gateway server that
16 is associated with the domain indicated by the user's user ID. The enterprise IM
17 gateway server may be configured to verify that the user is a valid user associated
18 with the enterprise and enforce one or more enterprise policies that may be
19 associated with the user and public instant message connection requests. For
20 example, certain enterprise employees may not be authorized to participate in
21 public instant message communications. Additionally, enterprise policy may
22 specify whether or not specific enterprise employees are authorized to establish
23 point-to-point communication connections as may be enabled by a public instant
24 message service.

1 [0009] After the enterprise IM gateway server verifies the user identity and
2 applies any associated enterprise policies, if the user is authorized, the enterprise
3 IM gateway server forwards the connection request to the public instant message
4 service with data indicating that the request is being submitted from the enterprise
5 IM gateway server. Upon authentication by the public instant message service of
6 the enterprise IM gateway server identity and the user identity, a connection is
7 established between the public instant message service and the user through the
8 enterprise IM gateway server.

9 [0010] Enterprise IM gateway server may be configured to log public instant
10 message communications in which the user participates in an enterprise IM data
11 log.

12 [0011] In yet another embodiment, an enterprise environment may include
13 multiple, geographically distributed enterprise IM gateway servers. Public IM
14 service connection requests are redirected to an enterprise routing service, which
15 then determines, based on a geographic location associated with the user, which of
16 the multiple, geographically distributed enterprise IM gateway servers to which
17 the connection request is to be redirected.

18 19 **BRIEF DESCRIPTION OF THE DRAWINGS**

20 [0012] Figure 1 is a block diagram that illustrates various instant message
21 communication configurations for which data may be logged.

22 [0013] Figure 2 is a block diagram that illustrates an exemplary environment in
23 which a public instant message service may log domain-specific communications.
24
25

1 [0014] Figure 3 is a block diagram that illustrates an exemplary environment in
2 which an enterprise instant message gateway server may be implemented to enable
3 logging of employee instant message communications.

4 [0015] Figure 4 is a block diagram that illustrates an exemplary environment in
5 which multiple firewalled enterprise instant message gateway servers may be
6 implemented to enable logging of employee instant message communications.

7 [0016] Figure 5 is a block diagram that illustrates an exemplary geographically
8 distributed enterprise environment in which enterprise instant message gateway
9 servers may be implemented to enable logging of employee instant message
10 communications.

11 [0017] Figure 6 is a block diagram that illustrates select components of an
12 exemplary public instant message service.

13 [0018] Figure 7 is a flow diagram that illustrates an exemplary method for re-
14 directing an instant message connection request from a public instant message
15 server to an enterprise instant message gateway server.

16 [0019] Figure 8 is a block diagram that illustrates select components of an
17 exemplary enterprise IM gateway server.

18 [0020] Figure 9 is a flow diagram that illustrates exemplary processing that
19 may be performed by the enterprise IM gateway server illustrated in Figure 8.

20 21 **DETAILED DESCRIPTION**

22 **Overview**

23 [0021] The embodiments described below allow enterprise management of
24 instant message (IM) communications initiated through a public instant message
25 system. When a user (using an IM client) requests a connection with a public IM

1 service, the service checks the domain associated with the user. If the domain is
2 identified as one for which connections are to be managed (to enable logging or
3 monitoring of IM communications), then a monitored connection between the user
4 and the public IM service is established.

5 **[0022]** In one implementation, the public IM service logs IM communications
6 in which a user associated with a particular domain participates. At regular
7 intervals (e.g., hourly, daily, or weekly), the data that is logged may then be
8 transferred to a server associated with the domain.

9 **[0023]** In another implementation, connection requests associated with a
10 particular domain that are received by the public IM service are redirected to an
11 IM gateway server that is associated with the domain. A monitored connection
12 between the user and the public IM service is then established through the IM
13 gateway server. The IM gateway server is then able to log IM communications
14 that pass through it.

15 **Instant Message Communication Configurations**

16 **[0024]** Figure 1 illustrates various connection configurations through which
17 instant message communications may be performed. The left side of Figure 1
18 illustrates an enterprise environment 102 implemented, for example, as a corporate
19 network, behind an enterprise firewall 104. The right side of Figure 1 illustrates a
20 public environment 106, such as the Internet.

21 **[0025]** Within the enterprise environment 102, an enterprise instant message
22 service 108 may be implemented to enable enterprise employees to communicate
23 within the enterprise network via IM. For example, enterprise IM service 108 may
24 be implemented using Microsoft's Live Communication Server to support instant
25 message communication using Microsoft's Windows Messenger client software.

1 Instant message communications between users connected to the enterprise IM
2 service 108 may be logged in enterprise IM data log 110. For example, assuming
3 enterprise environment 102 is associated with Microsoft Corporation and has
4 “microsoft.com” as an enterprise domain name, employees Jack 112 and Jill 114
5 may both log into enterprise IM service 108 (with user IDs jack@microsoft.com
6 and jill@microsoft.com, respectively) and participate in an IM conversation 116.
7 That conversation may be logged into enterprise IM data log 110 as an enterprise
8 communication. In the illustrated example, Jack 112 and Jill 114 may be logged
9 into the enterprise network in any number of ways, including but not limited to,
10 via a network workstation or via a virtual private network (VPN) connection.

11 **[0026]** Similarly, in the public environment 106, users may participate in IM
12 conversations via a public IM service 118, such as Microsoft’s .NET Messenger
13 Service. For example, two users not associated with the enterprise, Sue 120 and
14 Bob 122, may connect to public IM service 118 using user IDs sue@msn.com and
15 bob@hotmail.com, respectively. Because these two users have no association
16 with the enterprise (based on the domains specified in their user IDs), there is no
17 need to log a conversation 124 between these users. Alternatively, a company
18 employee, Tom 126 may be working from home or while traveling, and connect to
19 public IM service 118 using his work user ID, tom@microsoft.com. Tom 126
20 may then have a conversation 128 with Sue 120, who is not an enterprise
21 employee. Because Tom 126 is connected to public IM service 118 as an
22 enterprise employee (based on his user ID, tom@microsoft.com),
23 conversation 128 should be logged as an enterprise communication.

24 **[0027]** In addition to logging into an enterprise IM service 108 from work or
25 logging into a public IM service 118 from home, there may be times when an

1 employee connects to public IM service 118 from work. The employee may then
2 participate in instant message communications with other individuals who are
3 connected to the public IM service 118. For example, Jill 114 may connect from
4 work to public IM message service 118 and participate in an IM conversation 130
5 with Tom 126. Because Jill 114 and Tom 126 are both Microsoft employees, IM
6 conversation 128 should be logged as an enterprise communication. Similarly,
7 conversation 132 is between Jill 114 connected to the public IM service 118 from
8 work and Sue 120 connected to the public IM service 118 from another location.
9 Because Jill 114 is connected to the public IM service 118 as an enterprise
10 employee, conversation 132 should also be logged as an enterprise
11 communication.

12 **Public Logging of Instant Message Communications**

13 **[0028]** Figure 2 illustrates an exemplary environment in which one or more
14 domain data logs may be implemented as part of the public IM service 118 to
15 enable logging of domain-specific instant message communications that occur
16 through public IM service 118.

17 **[0029]** In the illustrated example, public IM service 118 includes IM connect
18 domain store 202 and IM connect domain data logs 204(1), 204(2), ..., 204(N).
19 IM connect domain store 202 stores data that identifies domains for which instant
20 message communications are to be logged. Each IM connect domain data log 204
21 is associated with a domain for which IM communications are to be logged, as
22 indicated by the data stored in IM connect domain store 202.

23 **[0030]** When a user requests a connection to public IM service 118 using an IM
24 client application 206, the service compares the user ID domain name with data
25 stored in IM connect domain store 202. If the user is associated with an IM

1 connect domain, then any IM conversations that the user participates in are logged
2 in the IM connect domain data log 204 that is associated with the user's domain.

3 [0031] The data that is logged may then be transferred to enterprise IM data
4 log 208, which resides on an enterprise network 210. In one implementation, an
5 enterprise server (not shown) may connect to and download data from the IM
6 connect domain store 204 that is associated with the enterprise. In an alternate
7 implementation, public IM service 118 may, at regular intervals, automatically
8 transmit to enterprise IM data log 208, any data that has been logged. Enterprise
9 IM data log 208 may be implemented in any number of ways, including, but not
10 limited to, as a database, an XML file, a collection of text files, etc.

11 **Enterprise Logging of Instant Message Communications**

12 [0032] Figure 3 illustrates an exemplary environment in which an enterprise
13 instant message gateway server may be implemented to enable logging of
14 enterprise-related instant message communications that occur through public IM
15 service 118.

16 [0033] In the illustrated example, an enterprise employee, Tom 126 uses an
17 instant messaging client application 302 on his home computer to send a
18 connection request 304 to public instant message service 118. Tom attempts to
19 connect using his work user ID, "tom@microsoft.com". Public IM service 118
20 compares the requesting user ID to data stored in IM connect domain store 306 to
21 determine whether or not the requesting user ID is associated with a domain for
22 which connections are to be re-directed.

23 [0034] If the domain associated with the requesting user ID (e.g.,
24 "microsoft.com") is identified in IM connect domain store 306, then public IM
25 service 118 issues a transfer command 308 back to the requesting instant

1 messaging client application 302. The transfer command 308 specifies an IP
2 address or domain name, along with a port number (or other type of identifier)
3 associated with an alternate location through which IM connection requests
4 associated with the requesting user's domain are to be submitted.

5 **[0035]** In the illustrated example, transfer command 308 identifies enterprise
6 IM gateway server 310, which is maintained by the enterprise with which the user
7 is associated. IM client application 302 then sends a connection request 312 to the
8 port and IP address identified in the transfer command, which in this example, is
9 enterprise IM gateway server 310.

10 **[0036]** Enterprise IM gateway server 310 examines the user ID associated with
11 the request to verify that the requesting user is indeed a valid user associated with
12 the enterprise domain. Enterprise IM gateway server 310 also determines what, if
13 any, enterprise policies are to be applied in relation to public IM conversations the
14 requesting user participates in. For example, some employees (e.g., management)
15 may be allowed to participate in public IM conversations while representing the
16 company while other employees are not allowed to participate in any public IM
17 conversations while representing the company. Other policies may indicate
18 whether or not a particular user is authorized to engage in point-to-point
19 conversations that may be enabled through the public IM service 118.

20 **[0037]** In the illustrated implementation, enterprise policies are stored in policy
21 and configuration data store 314. When enterprise IM gateway server 310
22 receives connection request 312, enterprise IM gateway server 310 verifies that the
23 user is a valid enterprise user and that the user, based on enterprise policy, is
24 allowed to participate in public IM conversations. For example, enterprise IM
25 gateway server 310 accesses policy and configuration data store 314 to verify that

1 the requesting user is a valid user associated with the enterprise and to identify any
2 enterprise policies associated with the user.

3 **[0038]** After verifying that the requesting user is a valid user associated with
4 the enterprise and verifying that, based on enterprise policy, the requesting user is
5 authorized to participate in public IM communications, enterprise IM gateway
6 server 310 submits a connection request 316 on behalf of the user to public IM
7 service 118. Connection request 316 includes an identifier that indicates that the
8 request is being submitted from enterprise IM gateway server 310.

9 **[0039]** Public IM service 118 then issues a first authentication challenge to
10 verify that the IM gateway server from which the request was received is a valid
11 IM gateway server, and also that it is an IM gateway server associated with the
12 enterprise indicated by the domain name portion of the user ID. After receiving a
13 valid response from enterprise IM gateway server 310, public IM service 118
14 issues a second authentication challenge to authenticate the client application 302
15 from which connection request 316 was received. Upon validation of both the
16 enterprise IM gateway server 310 and the client application 302, a connection is
17 established between public IM service 118 and instant messaging client
18 application 302 through enterprise IM gateway server 310.

19 **[0040]** Once the connection has been established, any instant message
20 communications in which Tom 126 participates are routed through enterprise IM
21 gateway server 310, which may be configured to extract and/or log data associated
22 with those communications in enterprise IM data log 318.

23 **[0041]** In addition to routing and logging instant message communications
24 between IM client application 302 and public IM message service 118, enterprise
25 IM gateway server 310 may also be configured to control whether or not the

1 connected user may participate in point-to-point communications, which may be
2 enabled through IM client application 302. For example, in the described
3 implementation, communications between IM client application 302 and public
4 IM service 118 include data that indicates whether or not IM client application 302
5 is configured to allow point-to-point communication. Enterprise IM gateway
6 server 310 may be configured to modify the point-to-point configuration data that
7 is sent from IM client application 302 to public IM service 118, effectively
8 changing the IM client application configuration to not allow point-to-point
9 communication.

10 **[0042]** In the illustrated example, enterprise IM gateway server 310, policy and
11 configuration data store 314, and enterprise IM data log 318 are controlled by the
12 enterprise. For security reasons, it is likely that the enterprise would prefer to
13 restrict access to one or more of those components. Accordingly, Figure 4
14 illustrates an exemplary implementation in which an enterprise instant message
15 gateway server may be implemented behind a firewall to enable logging of
16 enterprise-related instant message communications that occur through public IM
17 service 118.

18 **[0043]** In the illustrated example, policy and configuration data store 314 and
19 enterprise IM data log 318 are implemented behind enterprise firewall 104(a). The
20 illustrated example also includes two enterprise IM gateway servers – enterprise
21 IM gateway server 402, which is implemented behind enterprise firewall 104(a);
22 and enterprise IM gateway server 404, which is implemented in what is known as
23 the “demilitarized zone” (DMZ) between enterprise firewall 104(a) and enterprise
24 firewall 104(b). This implementation is designed to prevent unauthorized access
25

1 from the outside to enterprise-sensitive data stored in enterprise IM data log 318
2 and policy and configuration data store 314.

3 **[0044]** In the illustrated example, an enterprise employee, Tom 126 uses an
4 instant messaging client application 302 on his home computer to send a
5 connection request 304 to public instant message service 118. Public IM
6 service 118 compares the requesting user ID to data stored in IM connect domain
7 store 306 to determine whether or not the requesting user ID is associated with a
8 domain for which connections are to be re-directed.

9 **[0045]** If the domain associated with the requesting user ID is identified in IM
10 connect domain store 306, then public IM service 118 issues a transfer
11 command 308 back to the requesting instant messaging client application 302.
12 The transfer command 308 identifies an alternate location through which IM
13 connection requests associated with the requesting user's domain are to be
14 submitted.

15 **[0046]** In the illustrated example, transfer command 308 identifies enterprise
16 IM gateway server 404, which is within DMZ 406 between enterprise
17 firewalls 104(a) and 104(b). IM client application 302 then sends a connection
18 request 312 to enterprise IM gateway server 404 (as indicated by the data included
19 in transfer command 308).

20 **[0047]** When enterprise IM gateway server 404 receives connection
21 request 312, enterprise IM gateway server 404 communicates with enterprise IM
22 gateway server 402 (which is located behind firewall 104(a)) to verify the user is a
23 valid enterprise user and that the user, based on enterprise policy, is allowed to
24 participate in public IM conversations. For example, enterprise IM gateway
25 server 404 may transmit the user ID associated with connection request 312 to

1 enterprise IM gateway server 402. Enterprise IM gateway server 402 then
2 accesses policy and configuration data store 314 to verify that the requesting user
3 is a valid user associated with the enterprise and to identify any enterprise policies
4 associated with the user. Any identified enterprise policies associated with the
5 requesting user are then transmitted from enterprise IM gateway server 402 to
6 enterprise IM gateway server 404.

7 **[0048]** After verifying that the requesting user is a valid user associated with
8 the enterprise and verifying that, based on enterprise policy, the requesting user is
9 authorized to participate in public IM communications, enterprise IM gateway
10 server 404 submits a connection request 316 on behalf of the user to public IM
11 service 118. Connection request 316 also includes an identifier that indicates that
12 the request is being submitted from enterprise IM gateway server 404.

13 **[0049]** As described above with reference to Figure 3, public IM service 118
14 then issues a first authentication challenge to verify that the IM gateway server
15 from which the request was received is a valid IM gateway server, and also that it
16 is an IM gateway server associated with the enterprise indicated by the domain
17 name portion of the user ID. After receiving a valid response from enterprise IM
18 gateway server 404, public IM service 118 issues a second authentication
19 challenge to authenticate the client application 302 associated with connection
20 request 316. Upon validation of both the enterprise IM gateway server 404 and
21 the client application 302, a connection is established between public IM
22 service 118 and instant messaging client application 302 through enterprise IM
23 gateway server 404.

24 **[0050]** Once the connection has been established, instant message
25 communications in which Tom 126 participates are routed through enterprise IM

1 gateway server 404, which may be configured to extract and/or log data associated
2 with those communications in enterprise IM data log 318.

3 [0051] An alternate implementation may not include enterprise IM gateway
4 server 404 or enterprise firewall 104(b). Rather, connection request 304 may be
5 redirected to enterprise IM gateway server 402, which then verifies the requesting
6 user identity and passes the connection request on to public IM service 118, as
7 described above.

8 [0052] Another alternate implementation may include enterprise IM gateway
9 server 404, but not include enterprise IM gateway server 402. Rather, the tasks
10 described above as being performed by enterprise IM gateway server 402 are
11 performed by enterprise IM gateway server 404.

12 [0053] In yet another implementation, enterprise IM data log 318 and/or policy
13 and configuration data store 314 may be implemented within DMZ 406, rather
14 than behind enterprise firewall 104(a). Furthermore, enterprise IM data log 318
15 may be implemented as a component of enterprise IM gateway server 402 or
16 enterprise IM gateway server 404. Similarly, policy and configuration data
17 store 314 may be implemented as a component of enterprise IM gateway
18 server 402 or enterprise IM gateway server 404.

19 **Geographically Distributed Enterprise Logging of IM Communications**

20 [0054] Figure 5 illustrates an exemplary geographically distributed
21 environment in which enterprise instant message gateway servers may be
22 implemented to enable logging of enterprise-related instant message
23 communications that occur through public IM service 118.

24 [0055] In the illustrated example, an enterprise network includes a central
25 network (e.g., located at corporate headquarters) and a remote network (e.g.,

1 located at another corporate office in another geographic location). For example,
2 the central network may be located at an office in the United States while the
3 remote network may be located at an office in Europe. In the described
4 implementation, an enterprise-controlled routing service is used to route an
5 employee IM connection request through an enterprise IM gateway server that is
6 associated, geographically, with the employee.

7 **[0056]** For example, in the configuration illustrated in Figure 5, the central
8 enterprise network includes central enterprise IM gateway server 502, central
9 enterprise IM data log 504, central policy and configuration data store 506, and
10 central enterprise directory 508. Similarly, the remote enterprise network includes
11 remote enterprise IM gateway server 510, remote enterprise IM data log 512,
12 remote policy and configuration data store 514, and remote enterprise
13 directory 516.

14 **[0057]** Central enterprise IM gateway server 502 and remote enterprise IM
15 gateway server 510 are similar to enterprise IM gateway servers 310, 402, and
16 404, described above with reference to Figures 3 and 4. Central enterprise IM data
17 log 504 and remote enterprise IM data log 512 are similar to enterprise IM data
18 log 318 described above with reference to Figures 3 and 4. Central policy and
19 configuration data store 506 and remote policy and configuration data store 514
20 are similar to policy and configuration data store 314 described above with
21 reference to Figures 3 and 4.

22 **[0058]** In the illustrated example, central enterprise IM gateway server 502 also
23 includes IM routing service 518. In alternate implementations, however, IM
24 routing service 518 may be implemented as a component of another enterprise
25 server, which may or may not be configured as an enterprise IM gateway server.

1 [0059] Central enterprise directory 508 maintains data that identifies for each
2 enterprise employee, an enterprise IM gateway server through which public IM
3 communications are to be routed. For example, central enterprise directory 508
4 may include a user ID, an IP address or DNS name, and a port number for each
5 enterprise employee. For a user whose office is located at the enterprise
6 headquarters (e.g., in the United States), the IP address or DNS name and port
7 number may identify an enterprise IM gateway server that is associated with the
8 central office, such as central enterprise IM gateway server 502. Similarly, for a
9 user whose office is located at another enterprise office (e.g., in Europe), the IP
10 address or DNS name and port number may identify an enterprise IM gateway
11 server that is associate with the remote office, such as remote enterprise IM
12 gateway server 510.

13 [0060] In an alternate implementation, central enterprise directory 508 may be
14 implemented as part of central policy configuration data store 506. Similarly,
15 remote enterprise directory 516 may be implemented as part of remote policy
16 configuration data store 514.

17 [0061] IM routing service 518 is configured to determine which enterprise IM
18 gateway server a particular user should be routed through for public IM
19 communications. For example, IM routing service 518 examines data stored in
20 central enterprise directory 508 to determine which enterprise IM gateway server a
21 particular connection request should be routed through.

22 [0062] In an exemplary implementation, remote enterprise directory 516 and
23 central enterprise directory 508 are synchronized to ensure that central enterprise
24 directory 508 has an up-to-date list of employees and associated data.
25

1 [0063] The configuration illustrated in Figure 5 is merely one example
2 configuration of a geographically distributed enterprise network system. Other
3 configurations are also contemplated, similar to those described above with
4 reference to Figures 3 and 4.

5 [0064] To establish an instant messaging connection, an enterprise employee
6 submits an IM connection request 520 to public IM service 118 using an IM client
7 application 522. As described above with reference to Figure 3, public IM
8 service 118 issues a transfer command 524 back to IM client application 522. The
9 transfer command 524 directs IM client application 522 to submit a connection
10 request 526 to IM routing service 518.

11 [0065] IM routing service 518 then uses the user ID associated with connection
12 request 526 to look up data in central enterprise directory 508 to determine
13 whether or not to issue a transfer command IM client application 522. If the data
14 in central enterprise directory 508 indicates that the user is associated with central
15 enterprise IM gateway server 502, then IM routing server 518 passes connection
16 request 526 to central enterprise IM gateway server 502, and processing continues
17 as described above with reference to Figures 3 and 4.

18 [0066] On the other hand, if the data in central enterprise directory 508
19 indicates that the user is associated with remote enterprise IM gateway server 510,
20 then IM routing server 518 issues a transfer command 528 to IM client
21 application 522, indicating that the connection is to be established through remote
22 enterprise IM gateway server 510.

23 [0067] IM client application 522 then submits connection request 530 to remote
24 enterprise IM gateway server 510. Processing then continues in a manner similar
25 to that described above with reference to Figures 3 and 4. An instant messaging

1 connection may be established between IM client application 522 and public IM
2 service 118 through remote enterprise IM gateway server 510. Whether or not the
3 connection is established, and specific parameters of the connection (e.g., which, if
4 any, point-to-point connections are allowed) may be based on data that remote
5 enterprise IM gateway server 510 extracts from remote policy and configuration
6 data store 514. If the connection is established, remote enterprise IM gateway
7 server 510 may be configured to log any public IM communications in remote
8 enterprise IM data log 512.

9 **[0068]** Although not illustrated, central policy and configuration data store 506
10 and remote policy and configuration data store 514 may be synchronized on a
11 regular basis. Similarly, central enterprise IM data log 504 and remote enterprise
12 IM data log 512 may also be synchronized. Alternatively, rather than
13 synchronizing, data stored in either remote policy and configuration data store 514
14 or remote enterprise IM data log 512 may be uploaded at regular intervals to
15 central policy and configuration data store 506 or central enterprise IM data
16 log 504, respectively. By doing so, a complete data log or policy store may be
17 maintained on the central enterprise network.

18 **Public IM Service Components**

19 **[0069]** Figure 6 illustrates select components of an exemplary public IM
20 service 118. In the illustrated example, public IM service 118 includes one or
21 more dispatch servers 602, one or more connection servers 604, one or more
22 switchboard servers 606, one or more presence servers 608, and IM connect
23 domain store 610 (which corresponds to IM connect domain store 202 shown in
24 Figure 2 and IM connect domain store 306 shown in Figures 3 and 4).

1 **[0070]** Dispatch server 602 is responsible for re-directing IM connection
2 requests that are received from a user associated with an IM connect domain.
3 Dispatch server 602 receives a connection request, determines whether or not IM
4 connect is enabled for the domain associated with the request, and if so, issues a
5 transfer command, redirecting the request to an IM gateway server associated with
6 the domain. If the request is not from a user associated with an IM connect
7 domain or if the request is received through an enterprise IM gateway server
8 (indicating that it is a request that has already been redirected), then the connection
9 request is passed off to connection server 604.

10 **[0071]** Connection server 604 is responsible for establishing and maintaining a
11 user connection. Connection server 604 receives a connection request from
12 dispatch server 602 and authenticates the client application from which the
13 connection request was received, for example by issuing a challenge to which a
14 valid response must be returned. (If the connection request was received from an
15 IM gateway server, then connection server 604 also authenticates the IM gateway
16 server from which the connection request was received.) Once the connection is
17 established, connection server 604 monitors the connection.

18 **[0072]** Switchboard server 606 is responsible for receiving and routing IM
19 communications between two or more connected users.

20 **[0073]** Presence server 608 is responsible for maintaining states associated with
21 each IM user, and pushing that information to other IM users so that when a user
22 connects, they are able to see, for example, whether or not other users they have
23 identified as contacts are also connected.

24 **[0074]** As described above, IM connect domain store 610 maintains a list of
25 domains for which IM connections are to be redirected. IM connect domain

store 610 may also store data indicating domains for which public IM service connections are not to be allowed. More specifically, IM connect domain store 610 may include the following data fields:

<u>Field Name</u>	<u>Description</u>
Domain	Domain Name (e.g., "microsoft.com")
IM Connect Enabled	True or False – indicates whether or not connections associated with the domain are to be redirected.
Transfer IP Address	Redirection address associated with the domain.
Transfer Domain Name	Domain Name associated with system to which connections are to be redirected.
Port Number	Identifier associated with a port through which redirected connection requests are to be submitted.
Managed Namespace Authorization Enabled	True or False – indicates whether or not non-redirection connections associated with the domain are to be allowed (e.g., in the case where the IM connect enabled field has a value of "False").
IM ID/Key Pair	Unique identifier associated with the enterprise that is represented by the domain.

IM Connection Redirection

[0075] Figure 7 is a flow diagram that illustrates an exemplary method 700 for managing requests for connections to a public IM service. The illustrated process can be implemented in any suitable hardware, software, firmware or combination thereof. Figure 7 is described for example purposes with respect to components shown in Figures 3 and 6.

[0076] At block 702, a public IM service receives a connection request. For example, dispatch server 602 may receive a connection request specifying a user ID (e.g., tom@microsoft.com) from IM client application 302. Alternatively, dispatch server 602 may receive a connection request from enterprise IM gateway

1 server 310 specifying a unique identifier that indicates that the connection request
2 is being received from a particular enterprise IM gateway server. For example, in
3 one implementation, a string that is a concatenation of a name of a company that
4 produced the IM gateway server and a domain name associated with the enterprise
5 may be used as a unique enterprise IM gateway server identifier.

6 **[0077]** At block 704, the public IM service determines whether or not the
7 request is being received from an IM gateway server. Dispatch server 602
8 examines data included with the connection request to determine whether or not an
9 enterprise IM gateway server is specified. For example, in the described
10 implementation, when enterprise IM gateway server 310 receives a redirected
11 connection request, enterprise IM gateway server 310 adds data to the connection
12 request before passing it on to public IM service 118. The data that is added (e.g.,
13 a unique enterprise IM gateway server identifier as described above with reference
14 to block 702) identifies the enterprise IM gateway server 310 through which the
15 connection request is being passed.

16 **[0078]** If the request is being received from an IM gateway server (the “Yes”
17 branch from block 704), then at block 706, public IM service 118 initiates a
18 challenge/response to verify the IM gateway server identity. For example,
19 dispatch server 602 passes the connection request to connection server 604.
20 Connection server 604 then issues a challenge to enterprise IM gateway server 310
21 to which a valid response must be submitted.

22 **[0079]** At block 708, public IM service 118 determines whether or not the
23 identity of the IM gateway server has been verified. In the described
24 implementation, connection server 604 verifies that an IM gateway server
25 response to the challenge has been received and that it identifies the IM gateway

1 server as a valid IM gateway server associated with the domain specified by the
2 user ID.

3 **[0080]** If the IM gateway server identity is verified (the “Yes” branch from
4 block 708), then at block 710, the connection processing then continues as a
5 standard public IM connection, which is well known to those skilled in the art.
6 The standard IM connection processing includes a second challenge/response to
7 verify the identity of the requesting client application.

8 **[0081]** If, on the other hand, the IM gateway server identify is not verified (the
9 “No” branch from block 708), then at block 720, connection server 604 denies the
10 connection request.

11 **[0082]** If however, the request is not being received from an IM gateway server
12 (the “No” branch from block 704), then at block 712, the public IM service
13 determines whether or not the request is associated with an IM connect domain.
14 For example, dispatch server 602 parses the user ID associated with the
15 connection request to identify the domain name. Dispatch server 602 then
16 searches a list of domain names stored in IM connect domain store 610 for the
17 domain name associated with the connection request.

18 **[0083]** If the request is not associated with an IM connect domain (the “No”
19 branch from block 712), then at block 710, the connection processing continues as
20 a standard IM connection.

21 **[0084]** If however, the request is associated with an IM connect domain (the
22 “Yes” branch from block 712), then at block 714 the public IM service determines
23 whether or not IM connect is enabled for the specified domain. For example,
24 dispatch server 602 examines the “IM connect enabled” field in IM connect
25

1 domain store 610 to determine whether or not IM connect (i.e., connection
2 redirection) is enabled for the identified domain.

3 [0085] If IM connect is enabled for the specified domain (the “Yes” branch
4 from block 714), then at block 716 the public IM service issues a transfer
5 command to the requesting IM client application. In the described
6 implementation, the transfer command specifies an IP address (or DNS name) and
7 a port number to which connection requests associated with the specified domain
8 are to be re-directed.

9 [0086] If however, IM connect is not enabled for the specified domain (the
10 “No” branch from block 714), then at block 718 the public IM service determines
11 whether or not managed namespace authorization is enabled for the specified
12 domain, which means that non-redirectioned connections to the public IM service are
13 not allowed. For example, dispatch server 602 examines the “managed namespace
14 authorization enabled” field in IM connect data store 610 to determine whether or
15 not managed namespace authorization is enabled for the identified domain.

16 [0087] If managed namespace authorization is not enabled for the specified
17 domain (the “No” branch from block 718), then at block 710 processing continues
18 as a standard IM connection.

19 [0088] If however, managed namespace authorization is enabled for the
20 specified domain (the “Yes” branch from block 718), then at block 720 the public
21 IM service denies the requested connection.

22 **Enterprise IM Gateway Server Components**

23 [0089] Figure 8 illustrates select components of an exemplary enterprise IM
24 gateway server 802. Enterprise IM gateway server 802 is representative of
25 enterprise IM gateway servers 310, 402, 404, 502, and 510 illustrated in

1 Figures 3-5. In the illustrated example, enterprise IM gateway server 802 includes
2 a processor 804 and a memory 806. User verification server 808, enterprise policy
3 verification service 810, IM connection service 812, and IM communication
4 logging service 814 are specific components that may be stored in memory 806
5 and executed on processor 804. Although shown as software components stored
6 in memory, in alternative implementations, each of these components may be
7 implemented as hardware, software, firmware, or any combination thereof.

8 **[0090]** User verification service 808 is configured to receive an IM connection
9 request and verify that the requesting user is associated with the enterprise.

10 **[0091]** Enterprise policy verification service 810 is configured to apply any
11 enterprise policies associated with the requesting user in establishing a public IM
12 connection. For example, enterprise policy verification service 810 examines data
13 stored in policy and configuration data store 314 to determine whether or not the
14 requesting user is authorized to participate in public IM communications.
15 Furthermore, enterprise policy verification service 810 may also use data stored in
16 policy and configuration data store 314 to determine which, if any, point-to-point
17 services the requesting user is authorized to participate in.

18 **[0092]** Instant message connection service 812 is configured to establish a
19 connection to public IM message service 118 on behalf of the requesting user. For
20 example, instant message connection service 812 submits a connection request to
21 public IM service 812, and responds to authorization challenges that may be
22 issued as part of a establishing a public IM service connection.

23 **[0093]** Instant message communication logging service 814 is configured to log
24 any data communicated to or from the user through a public IM service connection
25

1 that is established between the user and the public IM service 118 through the
2 enterprise IM gateway server 310.

3 **Enterprise IM Gateway Server Processing**

4 **[0094]** Figure 9 is a flow diagram that illustrates an exemplary method 900 that
5 may be performed by an enterprise IM gateway server to enable logging of public
6 IM communications. The illustrated process can be implemented in any suitable
7 hardware, software, firmware or combination thereof. Figure 9 is described for
8 example purposes with respect to components shown in Figures 3 and 8.

9 **[0095]** At block 902, enterprise IM gateway server 310 receives a connection
10 request. For example, user verification service 808 may receive a re-directed
11 connection request specifying a user ID (e.g., tom@microsoft.com) from IM client
12 application 302.

13 **[0096]** At block 904, enterprise IM gateway server 310 verifies the requesting
14 user's identity. For example, user verification service 808 determines whether or
15 not the requesting user is associated with the enterprise.

16 **[0097]** If the user is not a valid user associated with the enterprise (the "No"
17 branch from block 904), then at block 906, user verification service 808 denies the
18 requested connection.

19 **[0098]** If on the other hand, the user verification service 808 determines that the
20 requesting user is a valid enterprise user (the "Yes" branch from block 904), then
21 at block 908, enterprise IM gateway server determines whether or not the
22 requesting user is allowed to establish a public IM connection. For example,
23 enterprise policy verification service 810 examines data stored in policy and
24 configuration data store 314 to determine what, if any, enterprise policies apply to
25 the requesting user.

1 **[0099]** If it is determined that the requesting user is not allowed to participate in
2 public IM communications (the “No” branch from block 908), then at block 906,
3 enterprise policy verification service 810 denies the connection request.

4 **[0100]** If, on the other hand, it is determined that the requesting user is allowed
5 to participate in public IM communications (the “Yes” branch from block 908),
6 then at block 910, enterprise IM gateway server 310 adds server identification
7 information to the connection request. For example, IM connection service 812
8 may add a unique string identifier associated with the enterprise IM gateway
9 server 310 to a particular portion of the connection request.

10 **[0101]** At block 912, the connection request is submitted to public IM
11 service 118. For example, IM connection service 812 submits the connection
12 request to public IM service 118.

13 **[0102]** At block 914, enterprise IM gateway server 802 handles a server
14 authentication challenge. For example, IM connection service 812 receives
15 challenge from public IM service 812, and the IM connection service 812
16 responds with a key or other piece of data that the public IM service is expecting
17 in response to the challenge.

18 **[0103]** At block 916, enterprise IM gateway server 802 handles a client
19 application authentication challenge. For example, IM connection service 812
20 receives a client application authentication challenge from public IM service 812.
21 In one implementation, IM connection service 812 may respond to the challenge
22 on behalf of the client application. In an alternate implementation, IM connection
23 service 812 may pass the authentication challenge through to the client
24 application, wait for a response, and then pass the response through to public IM
25 service 118.

1 [0104] At block 918, enterprise IM gateway server 802 passes through and logs
2 any IM communications that the user is participating in. For example, IM
3 connection service 812 controls the pass through of IM communications to or from
4 the user. As the communications are passed through enterprise IM gateway
5 server 802, IM communication logging service 814 logs data associated with the
6 IM communications, for example, in an enterprise IM data log.

7 Conclusion

8 [0105] The techniques described above enable enterprise management of public
9 instant message communications. Although the invention has been described in
10 language specific to structural features and/or methodological steps, it is to be
11 understood that the invention defined in the appended claims is not necessarily
12 limited to the specific features or steps described. Rather, the specific features and
13 steps are disclosed as preferred forms of implementing the claimed invention.